FortiClient (Windows) - Release Notes

Version 6.0.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

July 17, 2018
FortiClient (Windows) 6.0.0 Release Notes
04-600-480794-20180717

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-31	Initial release of FortiClient (Windows) 6.0.0.
2018-06-28	Added 499465 to Known Issues on page 22.
2018-07-10	Updated Special Notices on page 8.
2018-07-16	Updated Installation Information on page 12.
2018-07-17	Updated Upgrading from previous FortiClient versions on page 13.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.0 build 0067.

Review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

Microsoft Windows updates related to CPU security flaw (Meltdown)

Microsoft Windows updates may not occur due to a CPU security flaw (Meltdown) with anti-virus products installed. Please read the customer service bulletin CSB-180105-1 at https://support.fortinet.com/Information/Bulletin.aspx. A PDF of the bulletin can be downloaded from the firmware download directory of the Fortinet support site at https://support.fortinet.com.

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN 98% issues

The new SSL VPN Windows driver, which was first introduced in FortiClient 5.6.0, resolves various SSL VPN connection issues. The new driver will help increase performance by up to 20% and provide a stable VPN connection.

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, the login timeout on the FortiGate can be increased to 180 seconds using the following CLI command:

```
configure vpl ssl settings
   set log-in timeout 180
```

Windows notification of AV being disabled

In FortiClient 6.0.0, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopped running.

Local certificate store not supported

FortiClient (Windows) no longer supports the local certificate store, and it is recommended you use Windows Certificates Store instead. If you are currently using the local certificate store, you should transition to Windows Certificates Store before upgrading to FortiClient (Windows) 6.0.0.

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Rebranding tool not supported

FortiClient (Windows) 6.0.0 does not support the FortiClient Rebranding Tool.

What's New in FortiClient (Windows) 6.0.0

This section identifies the new features and enhancements in FortiClient (Windows) 6.0.0. For more information, see the *FortiClient Administration Guide*.

EMS quarantine file management

FortiClient 6.0 file quarantine functionality has been enhanced to support FortiClient EMS-based central quarantine management. This feature requires EMS 6.0.0.

User data security improvement

FortiClient user data security has been improved so user-specific saved information including the username, saved password, avatar, social ID and VPN information is not accessible to other users using the same device.

New FortiClient GUI

FortiClient 6.0.0 introduces a new UI that improves user experience and provides a refreshed look and feel. The new navigation bar provides up-to-date status information of all features while making them more accessible.

Improved Sandbox Detection techniques

Sandbox Detection has been enhanced in FortiClient 6.0 for better detection and interception of file transfers so files can be sent to FortiSandbox for behavior analysis.

Installed Software Inventory

FortiClient now sends all installed software application information to EMS so it display under Software Inventory. This feature requires EMS 6.0.0.

Customize system quarantine message

FortiClient can now display a customized quarantine message. This feature requires EMS 6.0.0.

FortiClient installs and runs as a 64-bit process on 64-bit platforms

FortiClient 6.0.0 now supports 64-bit installation.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientSetup_6.0.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.xx.xxxx.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
FortiClientSetup_6.0.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.xx.xxxx_x64.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
FortiClientTools_6.0.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN automation files

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	A virus cleaner
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS.
SSLVPNcmdline	Command line SSL VPN client
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools
VPNAutomation	A VPN automation tool

Review the following sections prior to installing FortiClient version 6.0.0: Introduction on page 6, Special Notices on page 8, and Product Integration and Support on page 15.

Installation options

When installing FortiClient version 6.0.0, you can choose the setup type that best suits your needs. By default, FortiClient always installs the Fortinet Security Fabric Agent (SFA) feature and enables the Vulnerability Scan feature. You can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

Upgrading from previous FortiClient versions

FortiClient version 6.0.0 supports upgrade from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Deploying FortiClient upgrades on Windows 7 endpoints via FortiClient EMS

When deploying FortiClient upgrades to Windows 7 endpoints via FortiClient EMS, the following steps are necessary to ensure a successful upgrade:

1. Install the Windows Update Hot Fix. Update to enable TLS 1.1 and TLS 1.2 as a default security protocol in WinHTTP (KB3140245): http://www.catalog.update.microsoft.com/search.aspx?q=kb3140245

   If regular Windows Update is enabled by default, this KB is already installed.

2. Create a DWORD registry entry: DefaultSecureProtocols in the path:
   x86 -
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
   x64 -
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
   Set the value to 0x00000A00 to enable both TLS 1.1 and 1.2.

See also https://support.microsoft.com/en-gb/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in.

Downgrading to previous versions

Downgrading FortiClient version 6.0.0 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 6.0.0 support

The following table lists version 6.0.0 product integration and support information.

FortiClient 6.0.0 support information

Desktop Operating Systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.0.0 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.0 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for FortiClient documentation • Windows Installer MSI installer version 3.0 or later.
FortiAnalyzer	• 6.0.0 • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.0.0

FortiManager	• 6.0.0 • 5.6.0 and later
FortiOS	• 6.0.0 and later • 5.6.0 and later Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • 5.4.0 and later
FortiSandbox	• 2.5.0 and later The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command: `device-authorization -f` • 2.4.0 and later The following supported versions do not offer authorization of FortiClient: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

FortiClient language support

Language	Graphical user interface	XML configuration	Documentation
English	✔	✔	✔
Chinese (simplified)	✔		
Chinese (traditional)	✔		
French (France)	✔		
German	✔		
Japanese	✔		
Korean	✔		
Portuguese (Brazil)	✔		
Russian	✔		
Spanish (Spain)	✔		

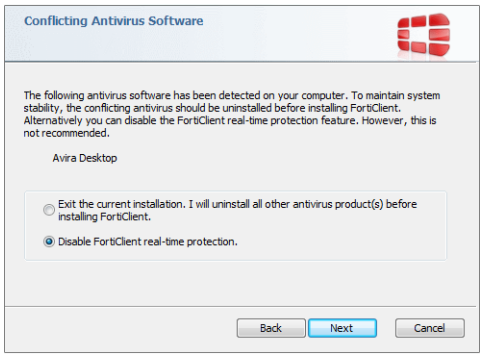
The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 6.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
448485	Change *onnet/offnet* status discovery for dual registration case.
458138	*onnet* status not being reported correctly on FortiClient when the EMS is offline.
460252	FortiESNAC was not able to detect the domain.
461004	EMS shows incorrect FortiClient state if EMS configured as both notification and management in IP list.
461405	FortiESNAC process stuck.
464911	EMS needs to re-sync profile to get AV events in.
465912	Endpoints disconnect randomly from EMS, still reporting themselves as being connected.
474993	FortiClient cannot be compliant when AV engine is different on FortiClient and FortiOS.
489943	FortiClient keeps on reregistering to FortiGate if it does not understand the error.
490182	FortiClient 6.0 compatibility with FortiOS 5.6.

Malware Protection

Bug ID	Description
411137	Cannot exclude UNC paths from scans.
421900	High CPU usage with *fmon.exe*.
443832	High CPU and freeze due to AV exclusions.
456910	No FortiSandbox scan for attachments in Windows 10 Mail app.
457439	AV real-time protection exclusion list with variables does not exclude all login users in terminal server.

Bug ID	Description
457445	*fmon* high CPU and big latency in Citrix server
459907	FortiClient 5.6.2 After switching FortiClient (Windows) AV off and then on again it no longer registers in Windows security center
460107	Client is blocking *Newly Observed Domains* but web filter categories are off.
460189	FortiClient does not run a full scan on USB insertion.
462162	Manual/right-click Sandbox scan does not increase file submitted count.
462704	Fortiae.exe failed to apply anti-exploit support list dynamically.
467324	Windows Meltdown patch compatibility.
470086	FortiShield stops protecting all files in FortiClient installation.
476218	Split *Block Malicious Websites* into subcategories.
484177	Windows context menu *Submit for analysis* does not send file.
489923	Sandbox exclusion list does not work with %userprofile% in Citrix environment.

Web Filter

Bug ID	Description
422496	Web Filter warn generate *utmevent=antivirus*.
445380	Add option to show block message from FortiClient (Windows) bubble popup for HTTPS site.
449279	FortiProxy blocks/prevents in-house software from working.
473247	Support new web filtering categories (9X) in FortiClient and EMS.

Application Firewall

Bug ID	Description
478677	*fortisniff2.sys* BSOD.
481597	*fortisniff2.sys* causing BSOD on several Windows 10 PCs using FortiClient (Windows) 5.6.6.

Remote Access

Bug ID	Description
409656	FortiClient removed default route of LTE card after connecting to IPsec VPN
451882	FortiClient (Windows) could be launched from SSL VPN web portal.
456320	SSL VPN saving password after unchecking *Always Up*.
461742	SSL_VPN on_connect script not working.
464651	FortiClient 5.6.0, 5.6.2, 5.6.3, 5.4.4 sometimes has slow download speed when connected to IPsec.
466486	FortiClient Windows VPN login forgery vulnerability.
469025	LogonUI.exe crashed caused by FortiCredentialProvider when VPN before logon enabled.
470706	Cannot connect to SSL VPN consistently with error code -20199.
473230	FortiClient *on_connect* script does not return correct password if contains special char %.
479097	SSL VPN is disconnected when using some application.
481115	*FortiSSLVPNclient.exe* triggers smart screen due to "unknown publisher".
481361	SSL VPN before logon does not appear on Windows 10 x64 after enabling even after reboot.
484368	FortiClient (Windows) could not access machine certificate when user logs into Windows as non-admin user when using IPsec VPN.

GUI

Bug ID	Description
462513	FortiGate should control option *Save Password* .
489453	*Site Violations* > *Clear Violations* does not work consistently.
489927	FortiClient Web Filter should display Security Risk categories once FortiClient (Windows) disabled antivirus feature.

Install and upgrade

Bug ID	Description
415585	Redeployment from EMS will reboot servers as no users logged in.
454184	Installing customized SSO only installer installed extra features.
460625	Delay in connecting to network after upgrade to 5.6.2.
467890	Minor upgrade breaks AV WSC integration.
480707	Installer crashes.
489136	EMS deployment does not work on Windows RS4 1803.
490359	FortiClient should support config firmware upgrade from FortiManager.

Other

Bug ID	Description
462455	*FCHelper64.ex*e causing error logs after upgrade to FortiClient (Windows) 5.6.2 on Windows 10.
464486	Revisit EPCUserAvatar.exe depency on .Net 3.5, 4.6.
464992	Avatar does not work properly on x64 Windows 8.1.
468993	FSSOMA always send default port 8001 no customized in Windows 7 x86.
473018	FortiClient SSO Mobility Agent Problem.
476108	FortiAvatar could not retrieve LinkedIn image anymore.
476110	FortiClient failed to change email address when user switched services.
478071	Unable to start a DCOM Server: the error: 740.
482124	Full translation of FortiClient to Korean.
488602	Typo in German translation.

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.0. For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
456917	Application Firewall became disabled when FortiClient was only monitored by EMS.
488095	EMS failed to update quarantined files for dual registered endpoint.
489256	Compliance with third party AV does not work properly .

Malware Protection

Bug ID	Description
480516	FortiClient AV ignoring exclusion list when AV scan is triggered by Windows scheduled task.
481003	FortiClient causing longer logon time to terminal server (Citrix) for first user.
483523	Black screen for a few minutes after login/logoff.
483806	User could still copy files on USB drive around with Sandbox enabled.
491199	FortiClient Sandbox right-click scan does not quarantine or block malicious file.

GUI

Bug ID	Description
472134	Some inconvenience with current per user password design for both SSL and IPsec.
475675	FortiClient dashboard reported wrong Sandbox status.
485558	*Fix Now* button shall be grayed out when there is no vulnerability.
485894	Differentiate stats message box and link for Sandbox.

Bug ID	Description
489159	If setting locked, clear button on notification page should be hidden.
489163	FortiTray cannot display VPN connection if "permission denied" box popup.
489228	FortiTray still showed to allow to connect other VPN tunnels when FortiClient was connecting one VPN.
489596	Windows should be minimized when VPN is up.
490222	*Save Password* should be selected if *Always Up* is selected.
490950	FortiClient always auto switch to corporate VPN when user tried to connect local configured VPN.
491270	*Save Password*, *Auto Connect*, *Always Up* do not show until refreshing the GUI after VPN is down.
491303	Password cannot be saved for auto-connect if there are multiple users.
491735	*Expand All* button has no effect.
491737	Manual scan shows scheduled scan is running.
491788	Redundant SSL VPN failed to connect will display IPsec error.
491842	For scheduled scans, default scan type should be full.
492210	Toggling *Block malicious websites* subcategory will not save the configuration.
492397	Connecting VPN from FortiTray should not list certificate.
492444	Right-click *Scan with FortiClient AntiVirus* window does not show progress dialog box.

Application Firewall

Bug ID	Description
450225	FortiClient blocking DNS when Application Firewall enabled.
477771	Add option to not block "unrated" if FortiGuard cannot be contacted.
482729	FortiClient blocking VM Horizon client as P2P/BitTorrent.
482920	Application Firewall blocking IPsec VPN DF set response.

Remote Access

Bug ID	Description
450245	Need to add a switch for the number of auto-connect retries.
467095	Wifi adapter failing to obtain an IP address after installing FortiClient.
475744	IPsec VPN keep running does not reconnect across network changes.
479236	FortiClient has issue with two factor authentication using Yubikey as 2FA for IPsec and SSL VPN.
480690	Default route is missing in FortiClient IPsec VPN.
486362	FortiClient disables Windows IKE and AuthIP IPsec Keying modules when connecting the VPN which effects MS direct access.
489066	SSL VPN password is being sent in reverse order when FortiClient (Windows) console run as non-administrator.
490855	Shows incorrect VPN profile when connect from FortiTray.
491407	IPsec VPN (with certificate) auto-connect when off-net not working if system did not restart between state change.
499465	SSL VPN custom host check for registry keys keeps failing on FortiClient 6.0.

Other

Bug ID	Description
476815	FortiClient reported remote server error when user selected LinkedIn service.
483945	Allow user to specify username on FortiClient console.
486330	Software Inventory - default Windows 10 programs not shown on EMS list.